What is claimed is:

1. An apparatus for encrypting/decrypting a real-time input stream, comprising:

a control unit receiving a data stream of byte units, converting the data stream into block data, and outputting the block data for encryption or decryption, the control unit receiving encrypted or decrypted block data, converting the received encrypted or decrypted block data into byte units, and outputting the converted block data of the byte units;

a key schedule unit carrying out a key schedule every round in accordance with a size and a key value of a block inputted from outside so as to output a key value for the encryption or decryption each round; and

a block round unit receiving converted data of block units from the control unit, receiving the key value from the key schedule unit so as to carry out the encryption or decryption, and outputting the encrypted or decrypted result to the control unit.

2. The apparatus of claim 1, the control unit comprising:

an input buffer storing the data stream of byte units and converting the received data stream into the block data

having a predetermined size so as to output the converted block data to the block round unit; and

an output buffer receiving the block data encrypted or decrypted in the block round unit and converting the received block data into the byte units so as to output a converted data.

3. The apparatus of claim 2, wherein the block round unit completes all round calculation of data having been currently encrypted or decrypted before a next block data is inputted from the control unit and then stores the corresponding result in the output buffer of the control unit.

4. The apparatus of claim 1, wherein the key schedule unit carries out in every round the key schedule on a key required for the block round unit to process each round so as to output the key scheduled result to the block round unit.

5. The apparatus of claim 4, the key schedule unit comprising:

a key expansion unit expanding the inputted key value into a size amounting to {block size * (count of rounds +1)}; and

a key selection unit selecting a 128 bits key required for each round from the expanded key value so as to output the selected key to the block round unit.

6. The apparatus of claim 1, wherein the key schedule unit expands the inputted key value into a size of {block size * (count of rounds + 1)} and then carries out a step of selecting the 128 bits key required for each round using one key register.

7. The apparatus of claim 6, wherein the key schedule unit comprises the key register amounting to the key value required substantially for one round.

8. The apparatus of claim 7, wherein the key register has a capacity amounting to {(size of an inputted block) * (size of one round)}.

9. The apparatus of claim 1, wherein the control unit generates a control signal to produce the key value

every round and then outputs the control signal to the key schedule unit.

10. An apparatus for encrypting/decrypting a real-time input data stream, comprising:

a control unit receiving a data stream in first data format, converting the data stream and outputting data in a second data format for encryption or decryption;

a key schedule unit in communication with the control unit and carrying out a key schedule every round in response to a size and a key value and outputting a key value for the encryption or decryption each round; and

a block round unit in communication with the control unit and the key schedule unit and receiving converted data in second data format from the control unit, receiving the key value from the key schedule unit so as to carry out at least one of the encryption or decryption, and outputting the encrypted or decrypted result to the control unit.

11. The apparatus of claim 10, wherein the first data format is in a byte unit, and the second data format is in a block unit.

12. The apparatus of claim 10, the control unit comprising:

an input buffer storing the data stream of the first data format and converting the received data stream into the data of the second data format having a predetermined size; and

an output buffer receiving data in the second data format and converting the data into the first data format.

13. The apparatus of claim 12, wherein the block round unit substantially completes all data encryption or decryption processing before a next set of data is inputted from the control unit and stores the corresponding result in the output buffer of the control unit.

14. The apparatus of claim 10, wherein the key schedule unit outputs a key schedule result in response to the key value to the block round unit in every round.

15. The apparatus of claim 14, the key schedule unit comprising:

a key expansion unit expanding the inputted key value into a size substantially equal to {second data format size * (count of rounds +1)}; and

a key selection unit selecting an N bit key required for each round from the expanded key value to output the selected key to the block round unit.

16. The apparatus of claim 15, wherein the N bit key is equal to a 128 bit key.

17. The apparatus of claim 10, wherein the key schedule unit expands the inputted key value into a size of {second data format size * (count of rounds + 1)} and then carries out a step of selecting an N bit key for each round.

18. The apparatus of claim 17, wherein the N bit key is equal to a 128 bit key.

19. The apparatus of claim 15, wherein the key schedule unit has a key register capable of processing the key value required substantially for one round.

20. The apparatus of claim 17, wherein a size of the key register is no less than {(second data format size) * (size of one round)}.

21. The apparatus of claim 10, wherein the control unit generates a control signal to produce the key value in every round.

22. A real-time encryption/decryption apparatus, comprising:

a control unit receiving a data stream in first data format, converting the data stream and outputting data in a second data format for encryption or decryption;

a key schedule unit in communication with the control unit and carrying out a key schedule in a predetermined period in response to a size and a key value, wherein the schedule unit has a key register capable of processing the key value required substantially for the predetermined period; and

a block round unit in communication with the control unit and the key schedule unit and receiving converted data in second data format from the control unit, receiving the key value from the key schedule unit so as to carry out at least one of the encryption or decryption.

23. The apparatus of claim 22, wherein the first data format is in a byte unit, and the second data format is in a block unit.

24. The apparatus of claim 22, wherein a size of the key register is no less than {(second data format size) * (size of one round)}.